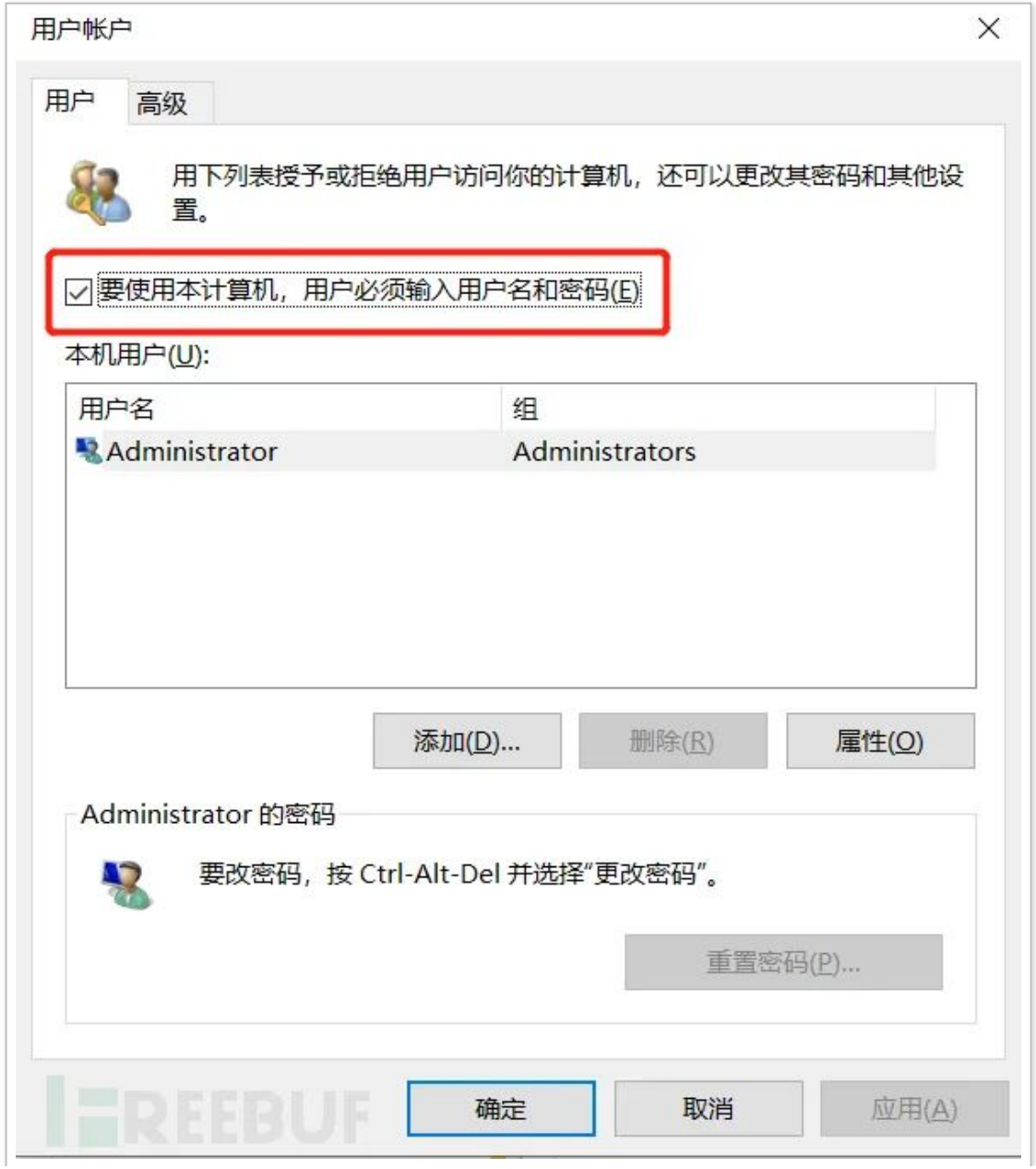
Windows 操作系统基线核查

一、身份鉴别

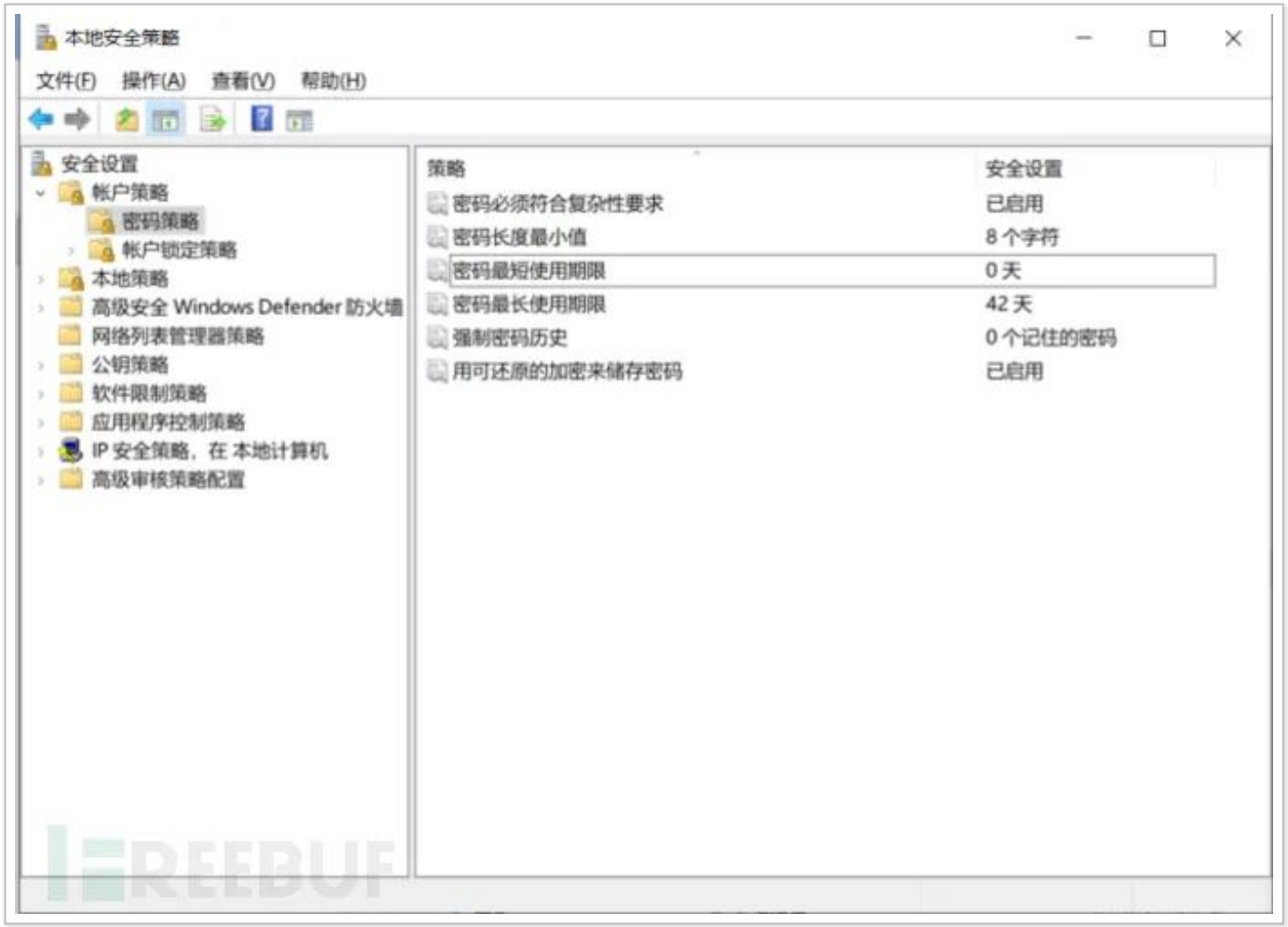
1.1 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换

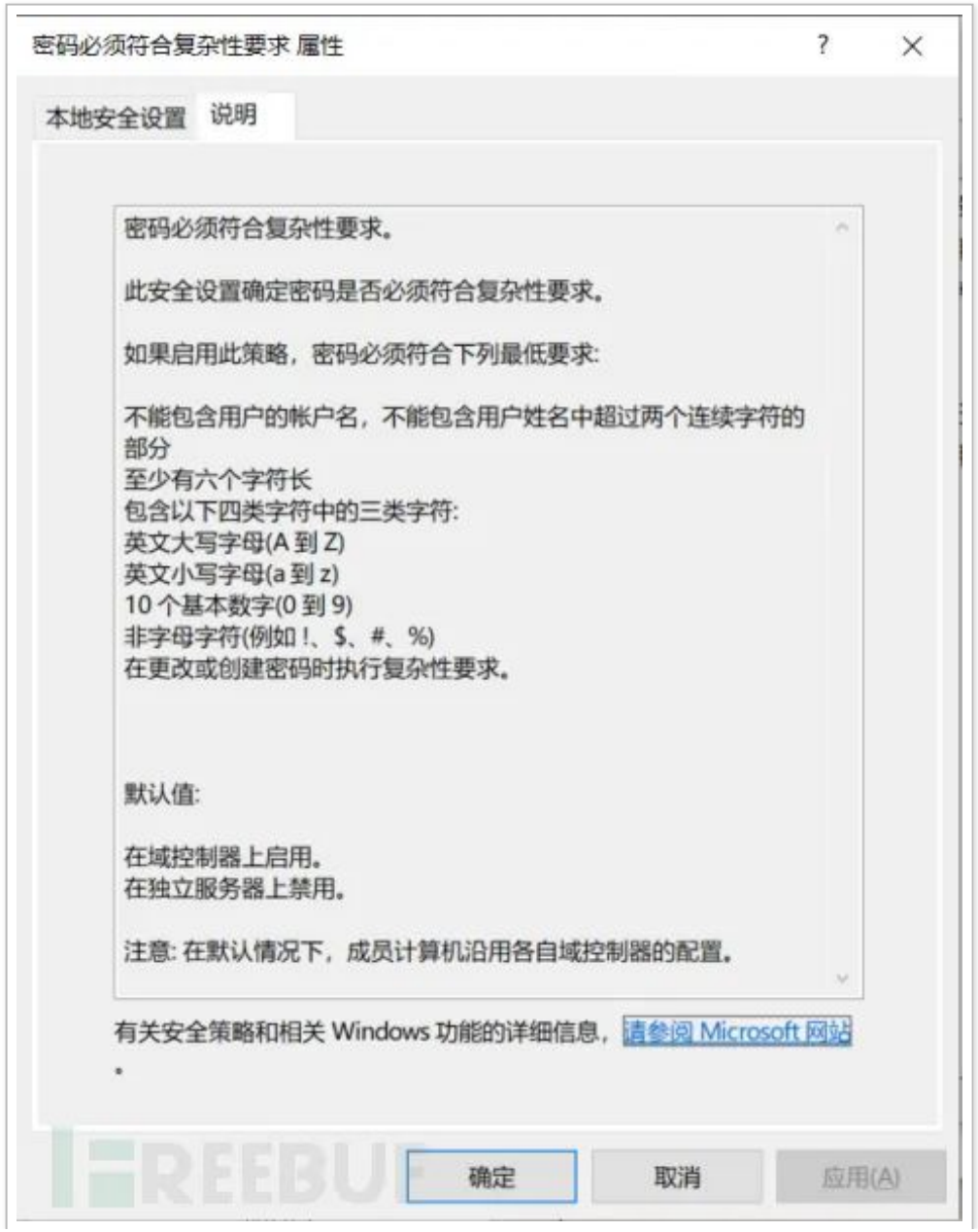
对用户进行鉴别也就是登录时需要你输入用户名、口令的行为。

针对本地登录，使用 Win+R 组合键打开运行框，在里面内输入 netplwiz，则会出现用户账户页面，如下所示：

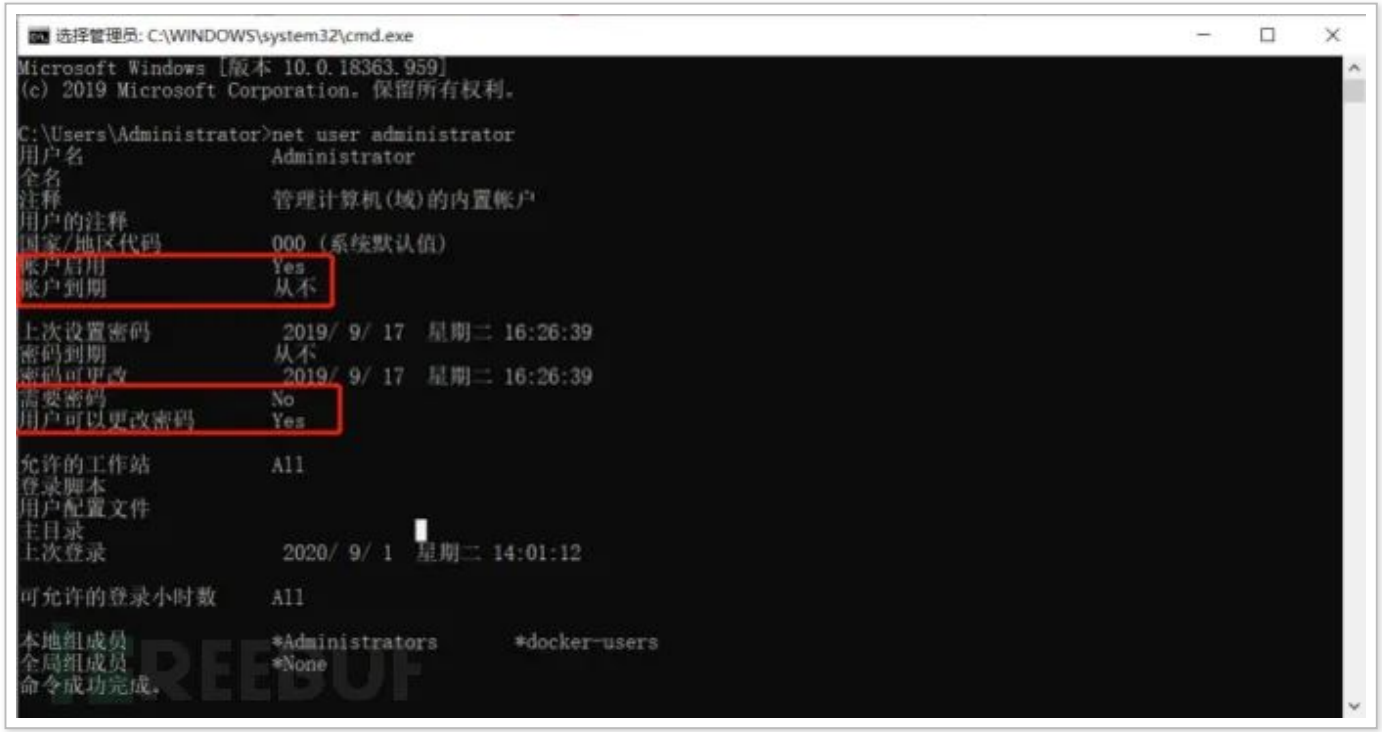

用户帐户
用户
高级
用下列表授予或拒绝用户访问你的计算机，还可以更改其密码和其他设置。
要使用本计算机，用户必须输入用户名和密码(E)
本机用户(U):
用户名
组
Administrator
Administrators
添加(D)...
删除(R)
属性(O)
Administrator 的密码
要改密码，按 Ctrl-Alt-Del 并选择"更改密码"。
重置密码(P)...
确定
取消
应用(A)

打开控制面板 -> 管理工具 -> 本地安全策略 -> 账户策略 -> 密码策略

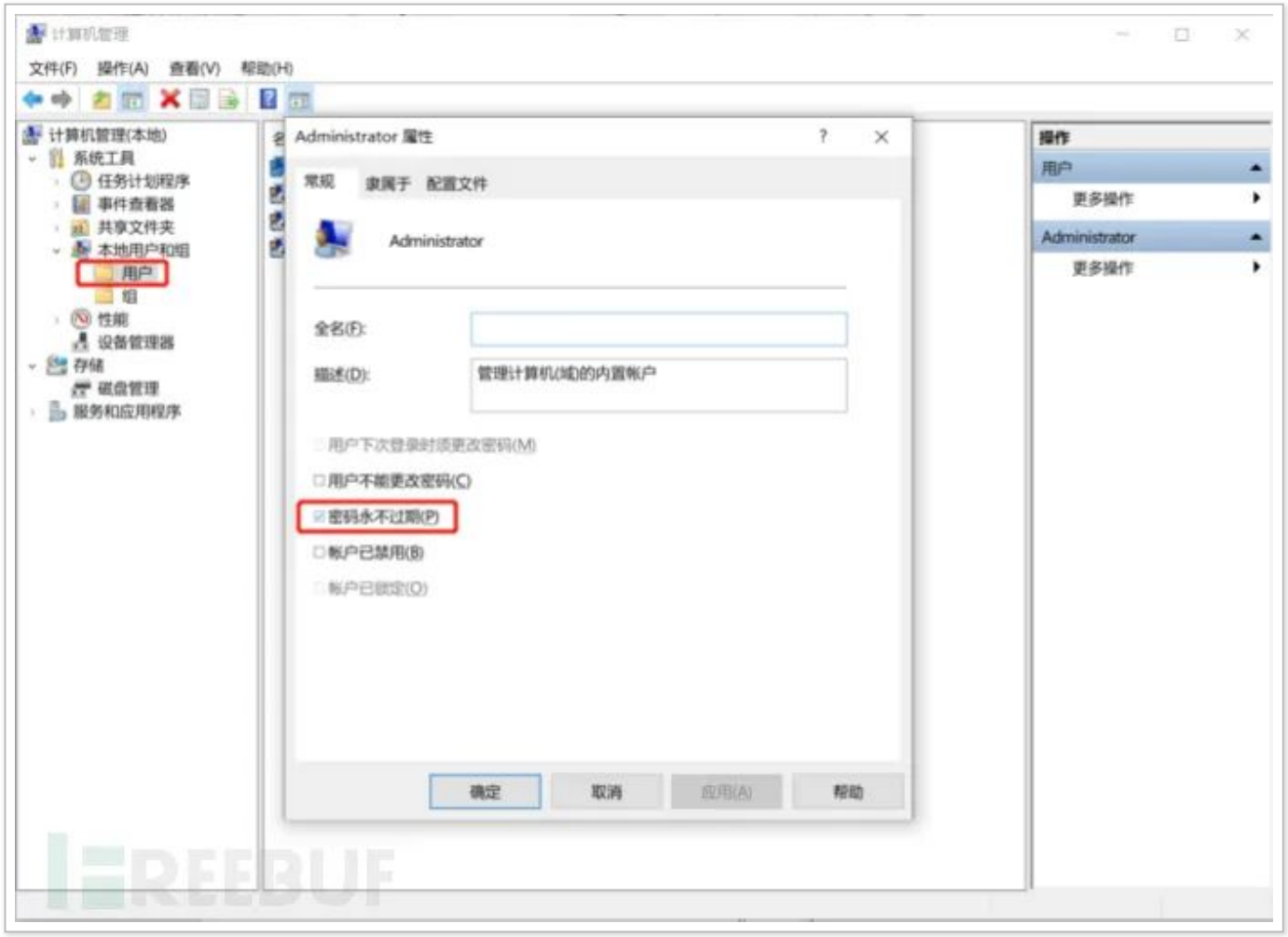



密码必须符合复杂性要求 属性
本地安全设置
说明
密码必须符合复杂性要求。
此安全设置确定密码是否必须符合复杂性要求。
如果启用此策略，密码必须符合下列最低要求:
不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分
至少有六个字符长
包含以下四类字符中的三类字符:
英文大写字母(A 到 Z)
英文小写字母(a 到 z)
10 个基本数字(0 到 9)
非字母字符(例如 !、$、#、%)
在更改或创建密码时执行复杂性要求。
默认值:
在域控制器上启用。
在独立服务器上禁用。
注意: 在默认情况下，成员计算机沿用各自域控制器的配置。
有关安全策略和相关 Windows 功能的详细信息，请参阅 Microsoft 网站
。
确定
取消
应用(A)

使用 Win+R 组合键打开运行框，在里面内输入 net user administrator，查看 administrator 账户更换密码的情况，加以证实。

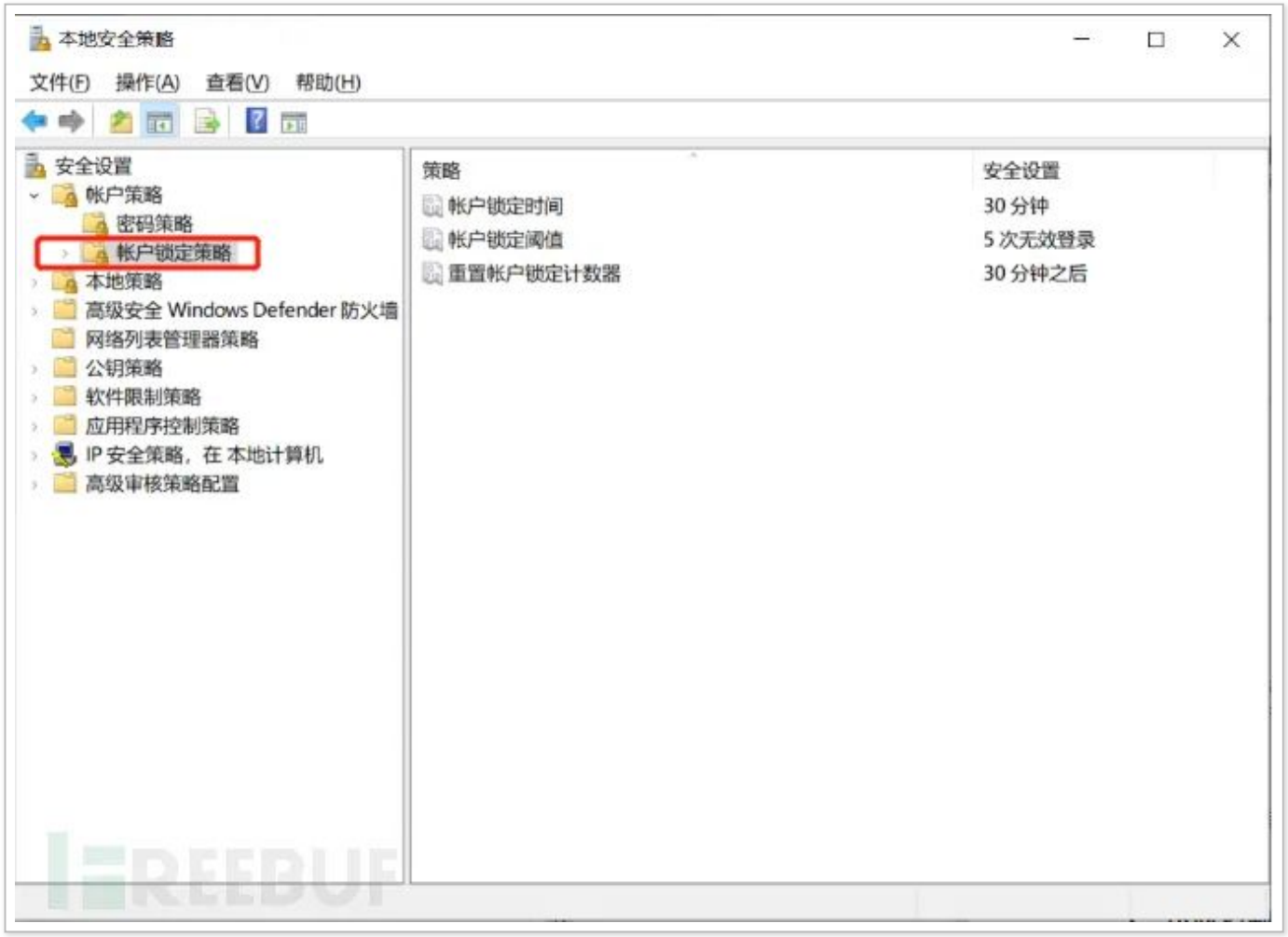


对于口令更换策略而言，还有个地方需要先去看看，也就是在计算机管理 - 本地用户和组 - 用户中，如果这里勾选了 “密码永不过期”，那么 windows 的密码策略中的“密码最长使用期限” 也就失效了。需要先把 “密码永不过期” 去掉。



1.2 应具有登录失败处理功能，应加固并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施

打开控制面板 -> 管理工具 -> 本地安全策略 -> 账户策略 -> 账户锁定策略

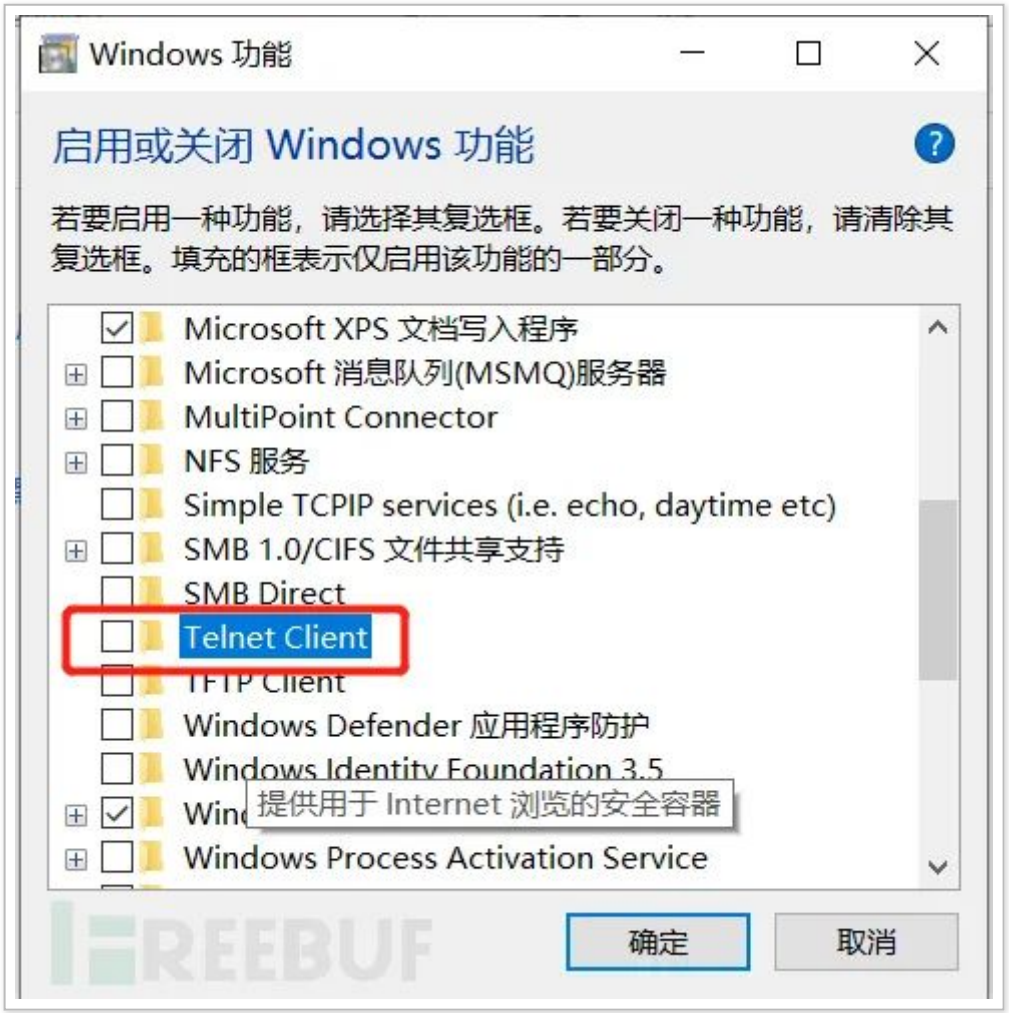


1.3 当进行远程管理时，应采取必要措施防止鉴别信息再网络传输过程中被窃听

如果被测评服务器没有连接外部网络，仅处于内网之中（也没有 wifi），管理服务器的方式就是跑去机房进行本地操作的话，也就不存在什么 “远程管理”，不存在什么 “数据保密性”，自然就符合了。

如果采用远程管理的方式，则分为使用远程桌面还是第三方软件。不可以直接使用远程桌面。同时也需要关闭 telnet 服务：

查看 telnet 服务是否开启，没有就合规。



建议采用 vpn 连接内网，然后通过堡垒机进行远程管理。

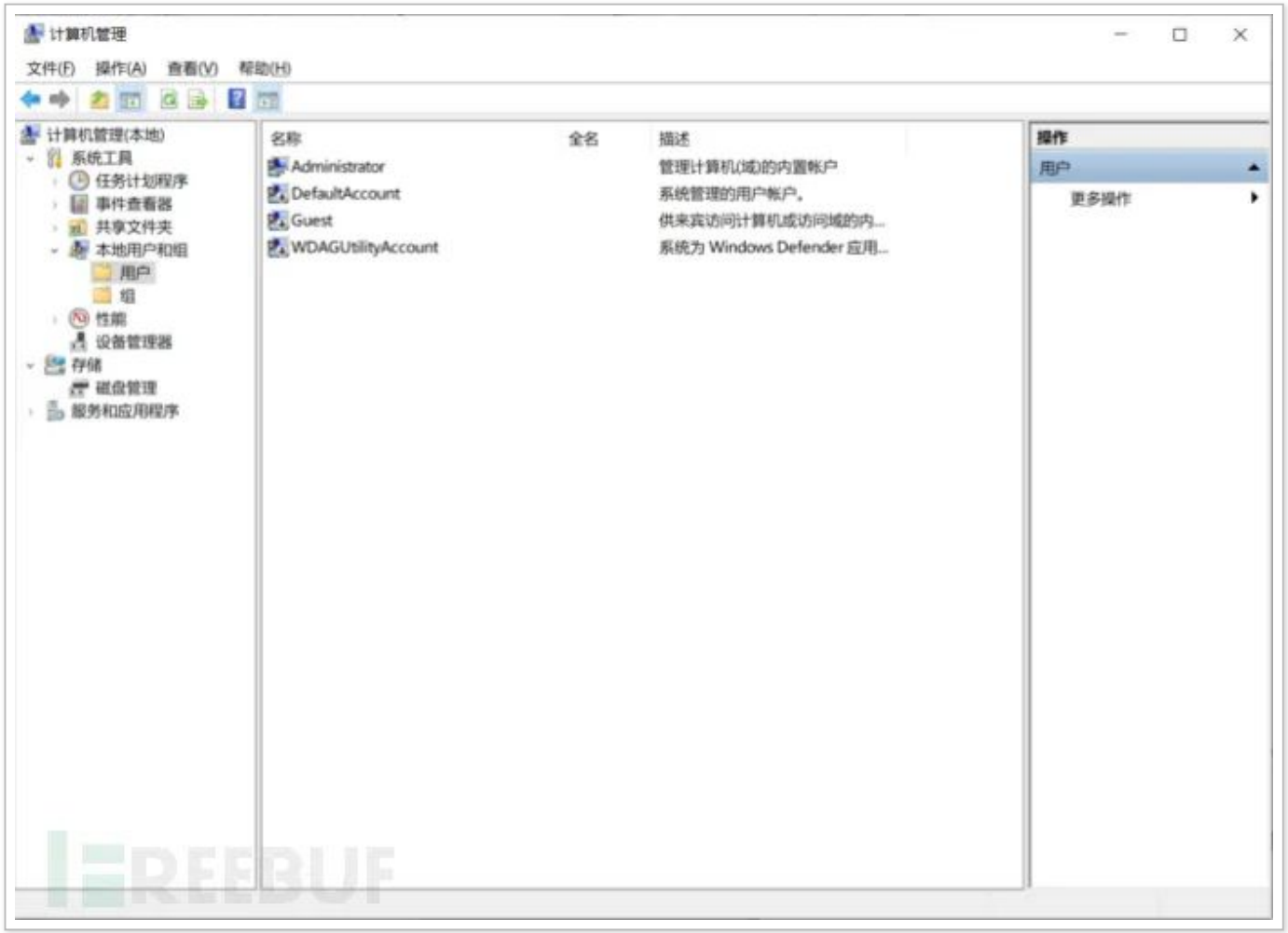
二、访问控制

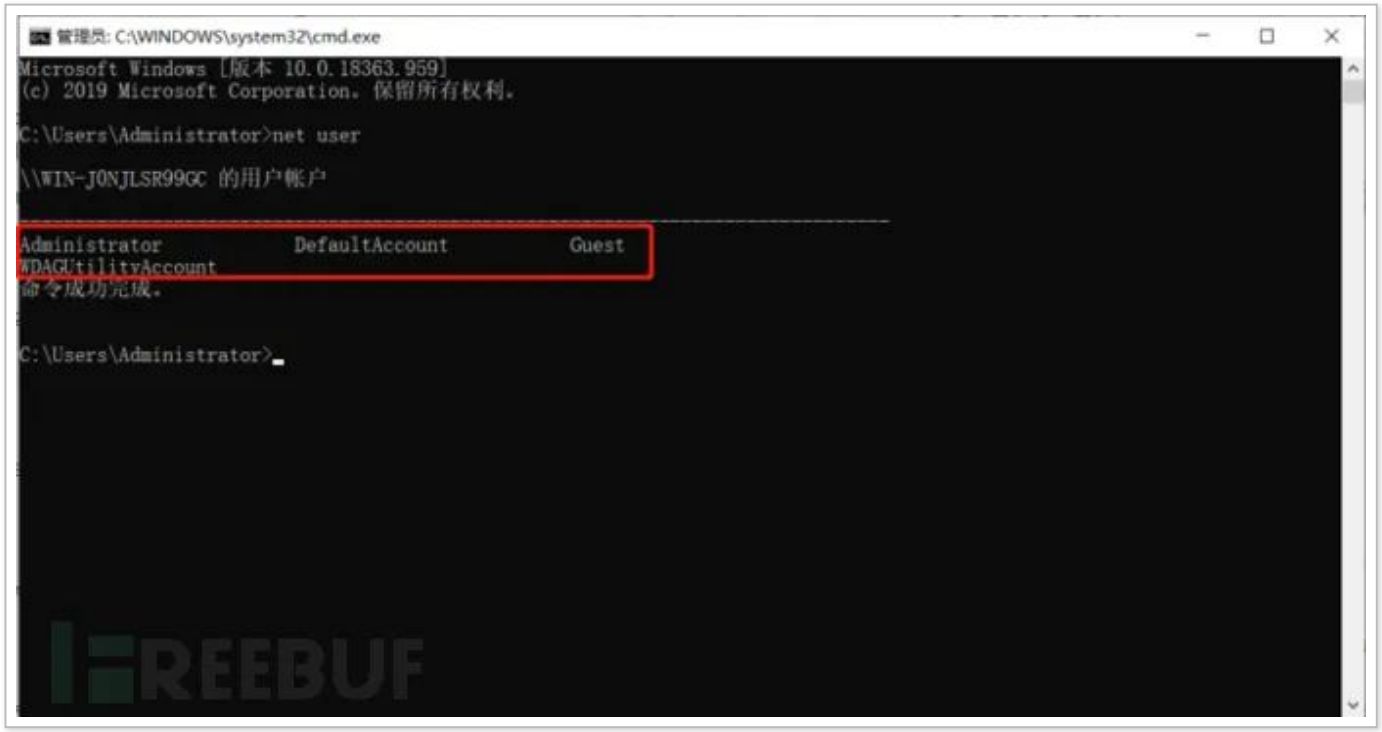
2.1 应对登录的用户分配账户与权限

如果 windows 系统中仅存在 Administrator 账户可用的话，就无所谓分配不分配了，无论谁来，都只能登录这一个账户，自然就不符合要求。建议建立几个普通用户，赋予在其正常工作范围内的操作权限。

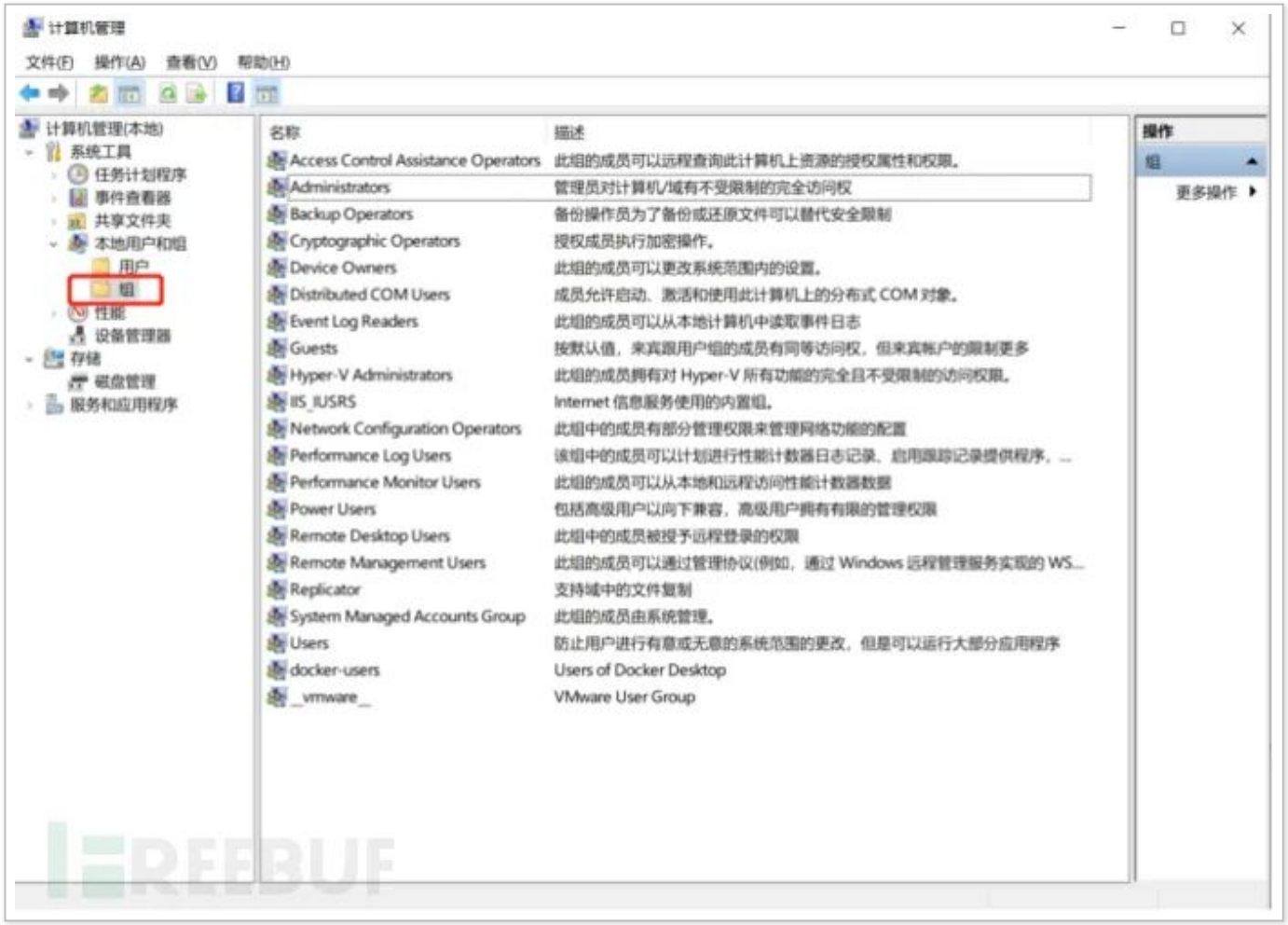
2.2 应重命名或删除默认账户，修改默认账户的默认口令

查看是否存在默认账户

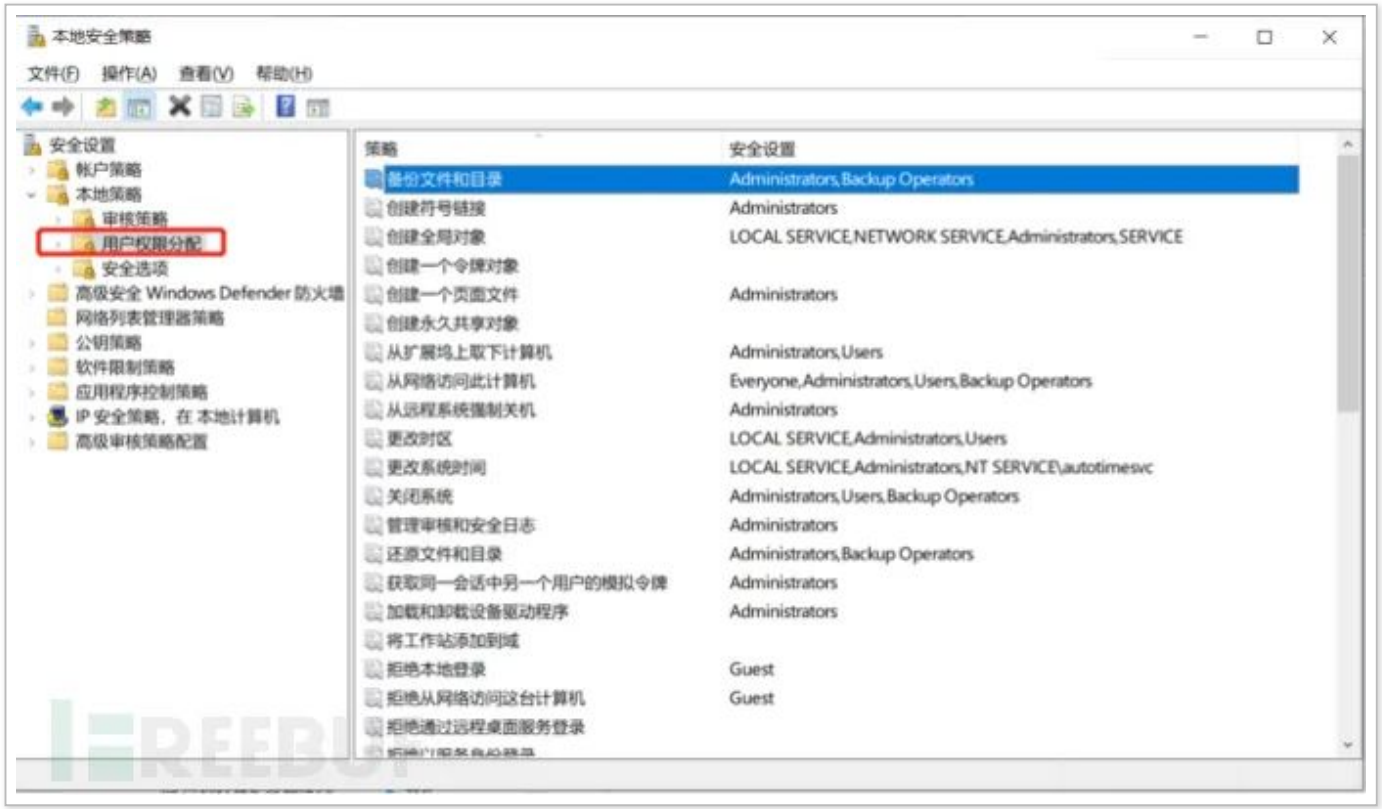

计算机管理
文件(F) 操作(A) 查看(V) 帮助(H)
计算机管理(本地)
系统工具
任务计划程序
事件查看器
共享文件夹
本地用户和组
用户
组
性能
设备管理器
存储
磁盘管理
服务和应用程序
名称
全名
描述
Administrator
管理计算机(域)的内置帐户
DefaultAccount
系统管理的用户帐户。
Guest
供来宾访问计算机或访问域的内...
WDAGUtilityAccount
系统为 Windows Defender 应用...
操作
用户
更多操作



同时查看 “组” 里面的用户和组的说明：

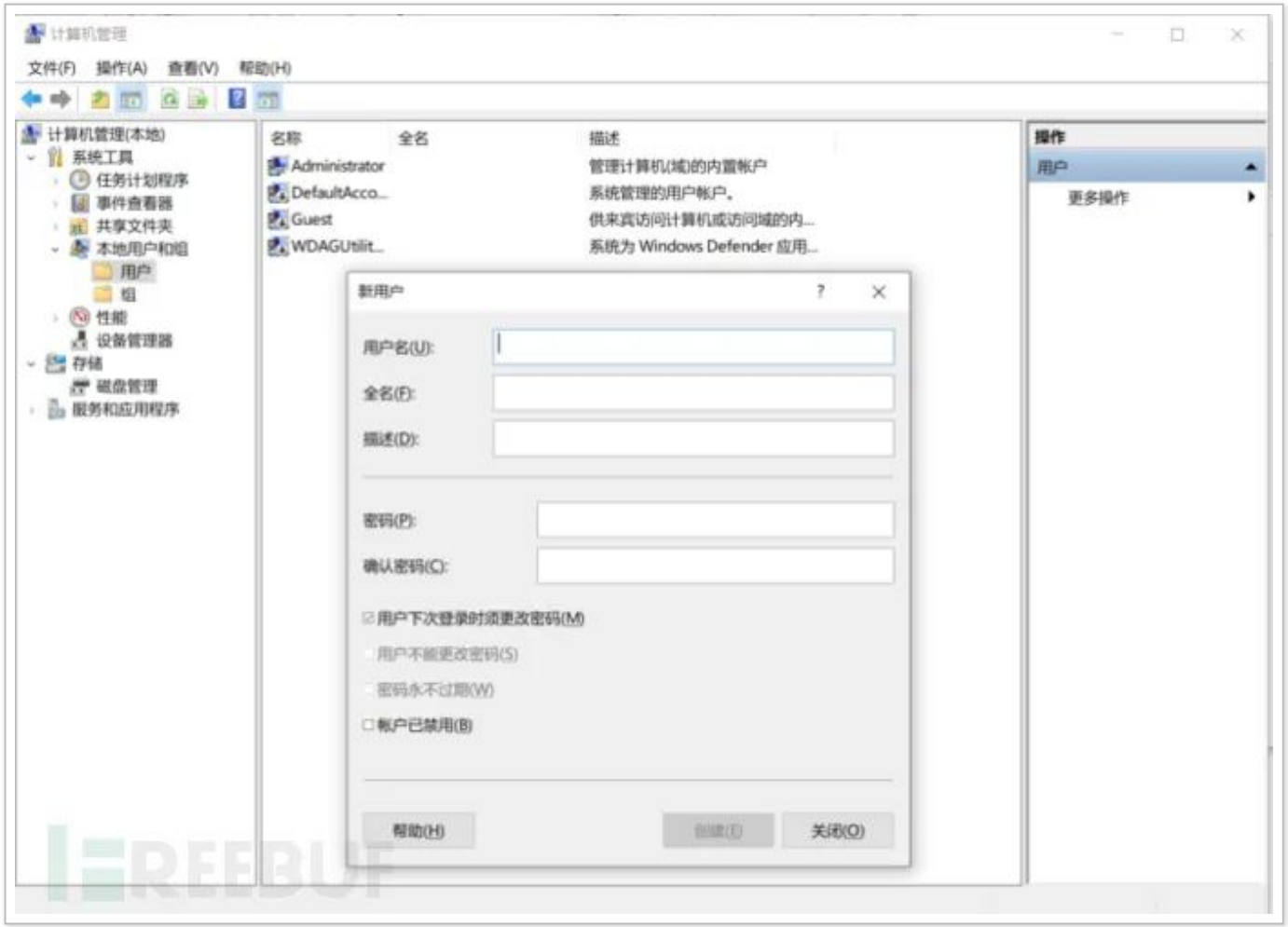

计算机管理
文件(F) 操作(A) 查看(V) 帮助(H)
计算机管理(本地)
系统工具
任务计划程序
事件查看器
共享文件夹
本地用户和组
用户
组
性能
设备管理器
存储
磁盘管理
服务和应用程序
名称
描述
Access Control Assistance Operators 此组的成员可以远程查询此计算机上资源的授权属性和权限。
Administrators 管理员对计算机/域有不受限制的完全访问权
Backup Operators 备份操作员为了备份或还原文件可以替代安全限制
Cryptographic Operators 授权成员执行加密操作。
Device Owners 此组的成员可以更改系统范围内的设置。
Distributed COM Users 成员允许启动、激活和使用此计算机上的分布式 COM 对象。
Event Log Readers 此组的成员可以从本地计算机中读取事件日志
Guests 按默认值，来宾跟用户组的成员有同等访问权，但来宾帐户的限制更多
Hyper-V Administrators 此组的成员拥有对 Hyper-V 所有功能的完全且不受限制的访问权限。
IIS_IUSRS Internet 信息服务使用的内置组。
Network Configuration Operators 此组中的成员有部分管理权限来管理网络功能的配置
Performance Log Users 该组中的成员可以计划进行性能计数器日志记录、启用跟踪记录提供程序，...
Performance Monitor Users 此组的成员可以从本地和远程访问性能计数器数据
Power Users 包括高级用户以向下兼容，高级用户拥有有限的管理权限
Remote Desktop Users 此组中的成员被授予远程登录的权限
Remote Management Users 此组的成员可以通过管理协议(例如，通过 Windows 远程管理服务实现的 WS...
Replicator 支持域中的文件复制
System Managed Accounts Group 此组的成员由系统管理。
Users 防止用户进行有意或无意的系统范围的更改，但是可以运行大部分应用程序
docker-users Users of Docker Desktop
__vmware__ VMware User Group
操作
组
更多操作

查看用户权限分配情况：



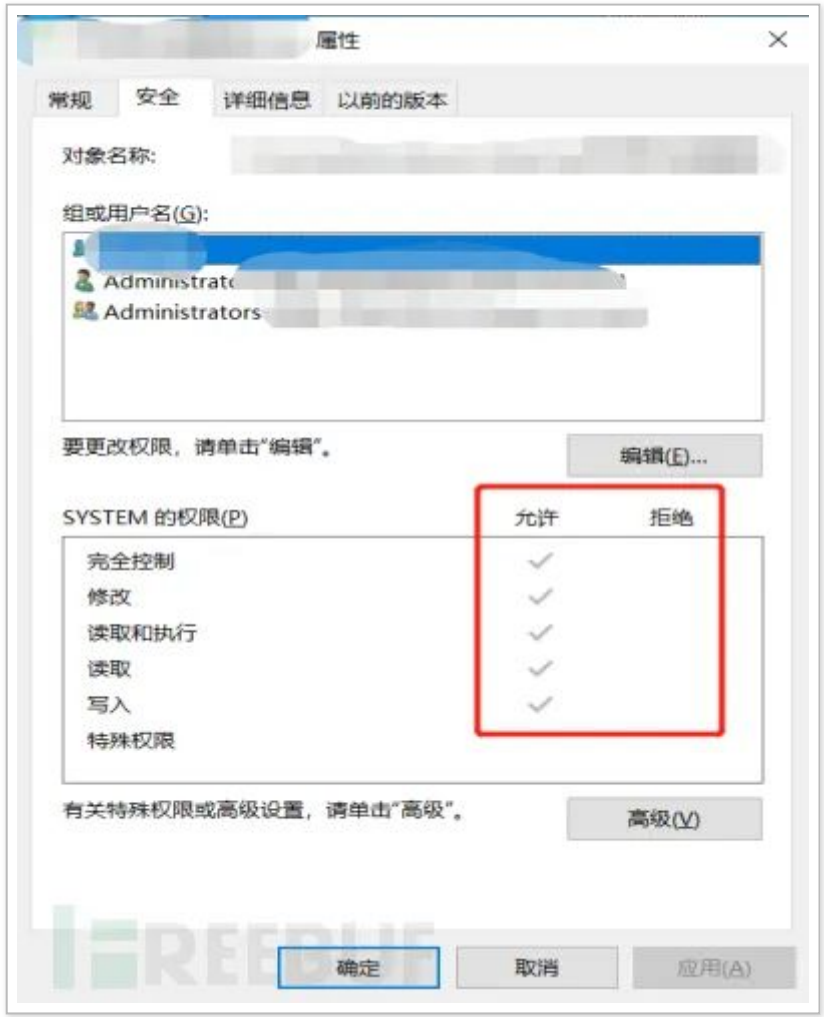
2.3 应及时删除或停用多余的、过期的账户，避免共享账户的存在

若只存在一个 administrator 账户，需要新建适量的新用户，确保避免共享账户的存在。若有多余、过期的账户，需要及时清理删除。



2.4 用授予管理用户所需的最小权限，实现管理用户的权限分离

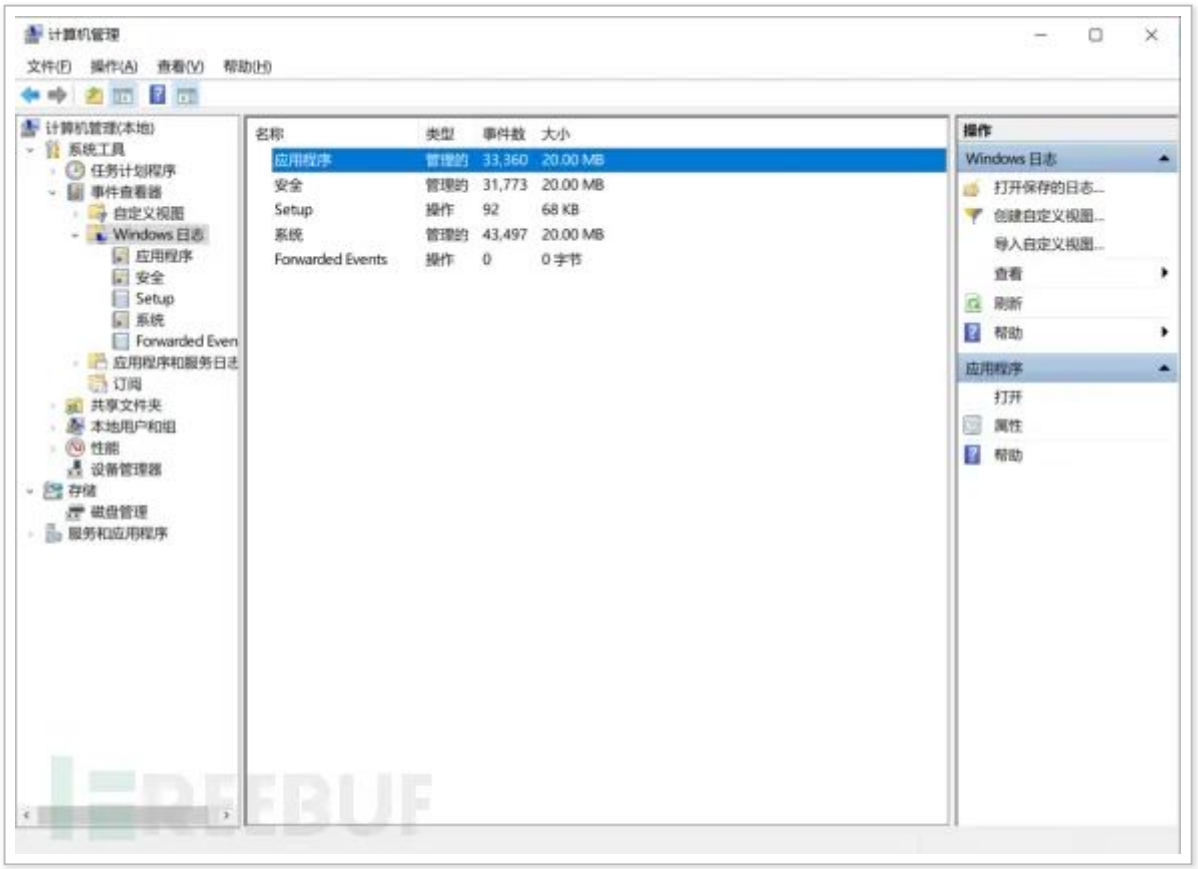
限制普通用户所需的最小权限，控制其访问范围

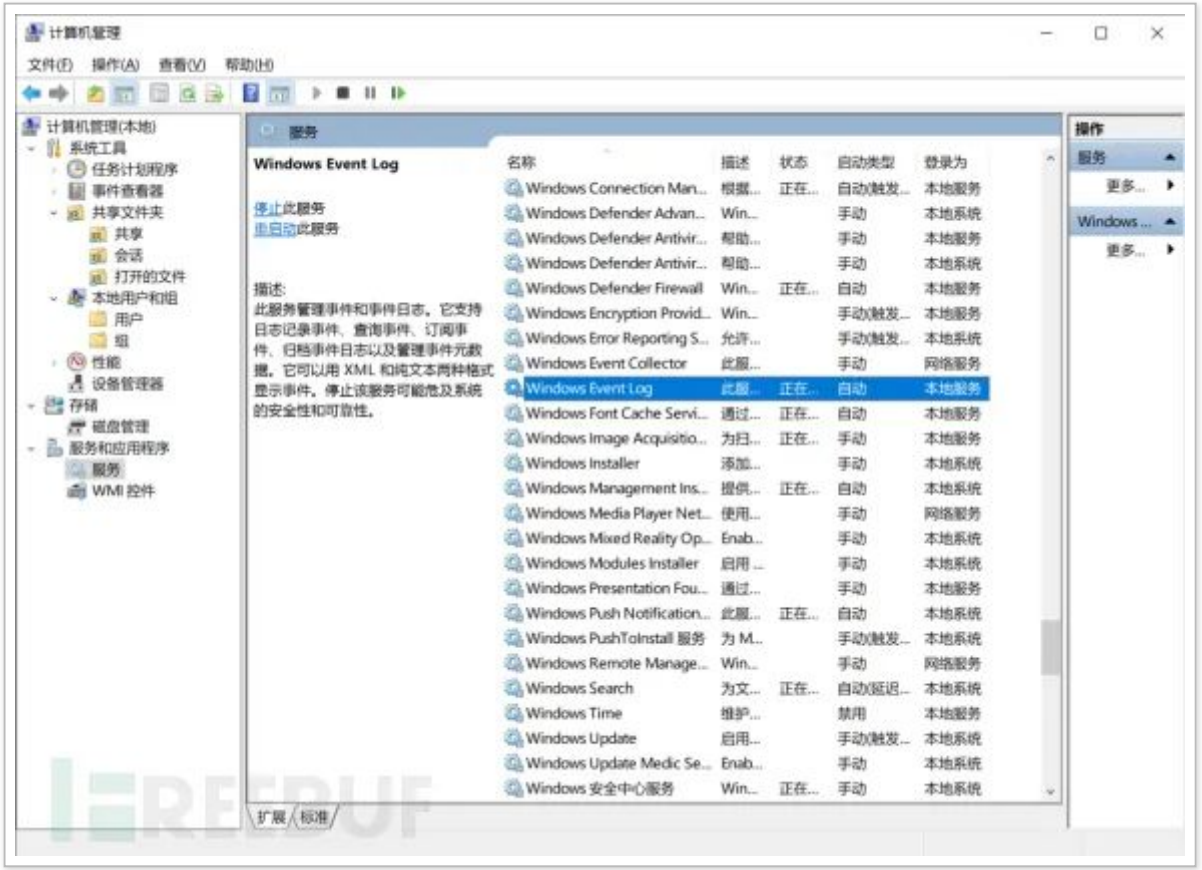

属性
常规
安全
详细信息
以前的版本
对象名称:
组或用户名(G):
Administrat
Administrators
要更改权限，请单击"编辑"。
编辑(E)...
SYSTEM 的权限(P)
允许
拒绝
完全控制
修改
读取和执行
读取
写入
特殊权限
有关特殊权限或高级设置，请单击"高级"。
高级(V)
确定
取消
应用(A)

三、安全审计

3.1 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计

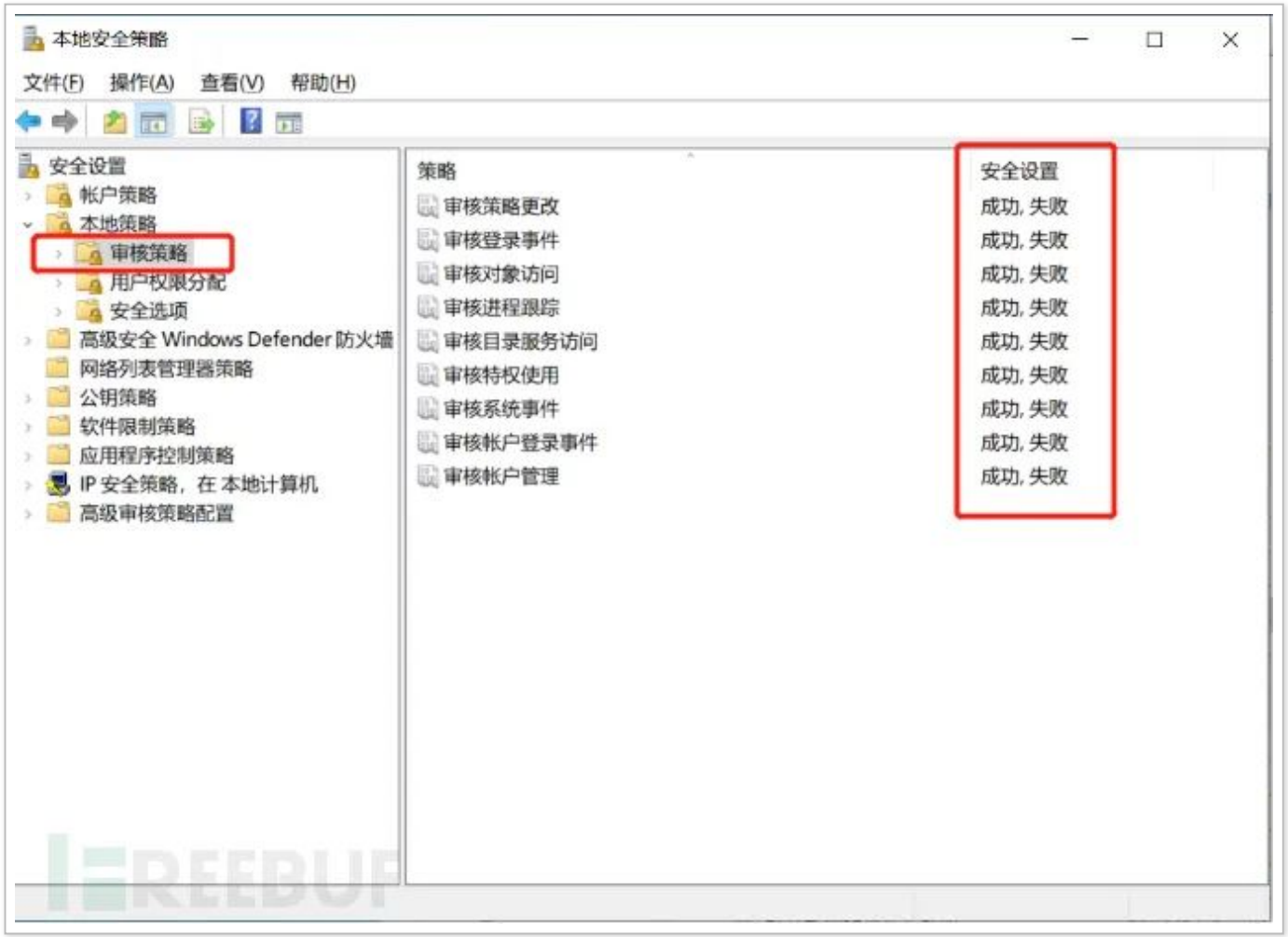
查看 windows 日志功能是否开启，默认一般都是开启状态





3.2 审计记录应包括事件的日期、用户、事件类型、事件是否成功及其它与审计相关的信息

查看审计策略，若不是下图这样，则不合规。

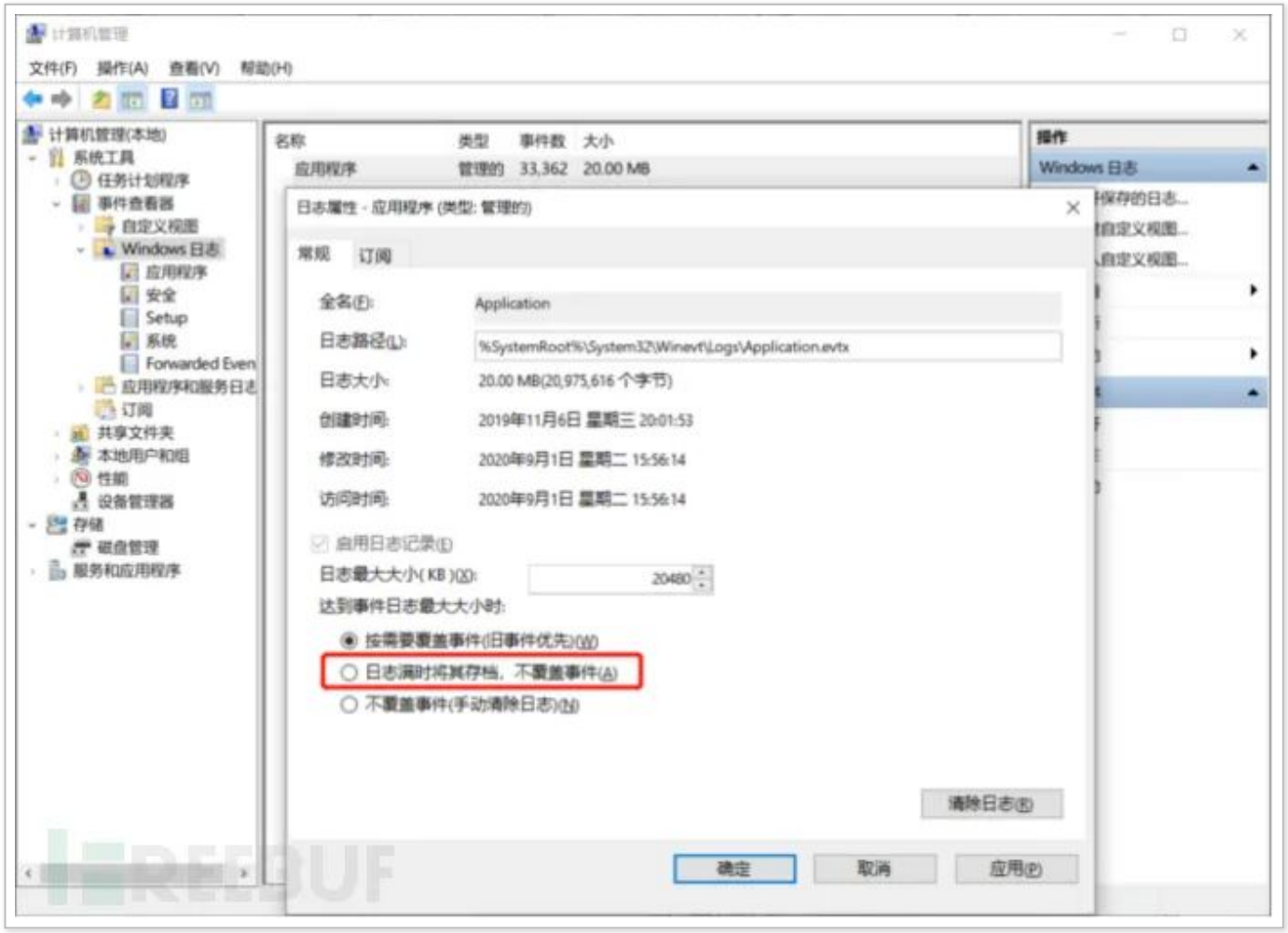


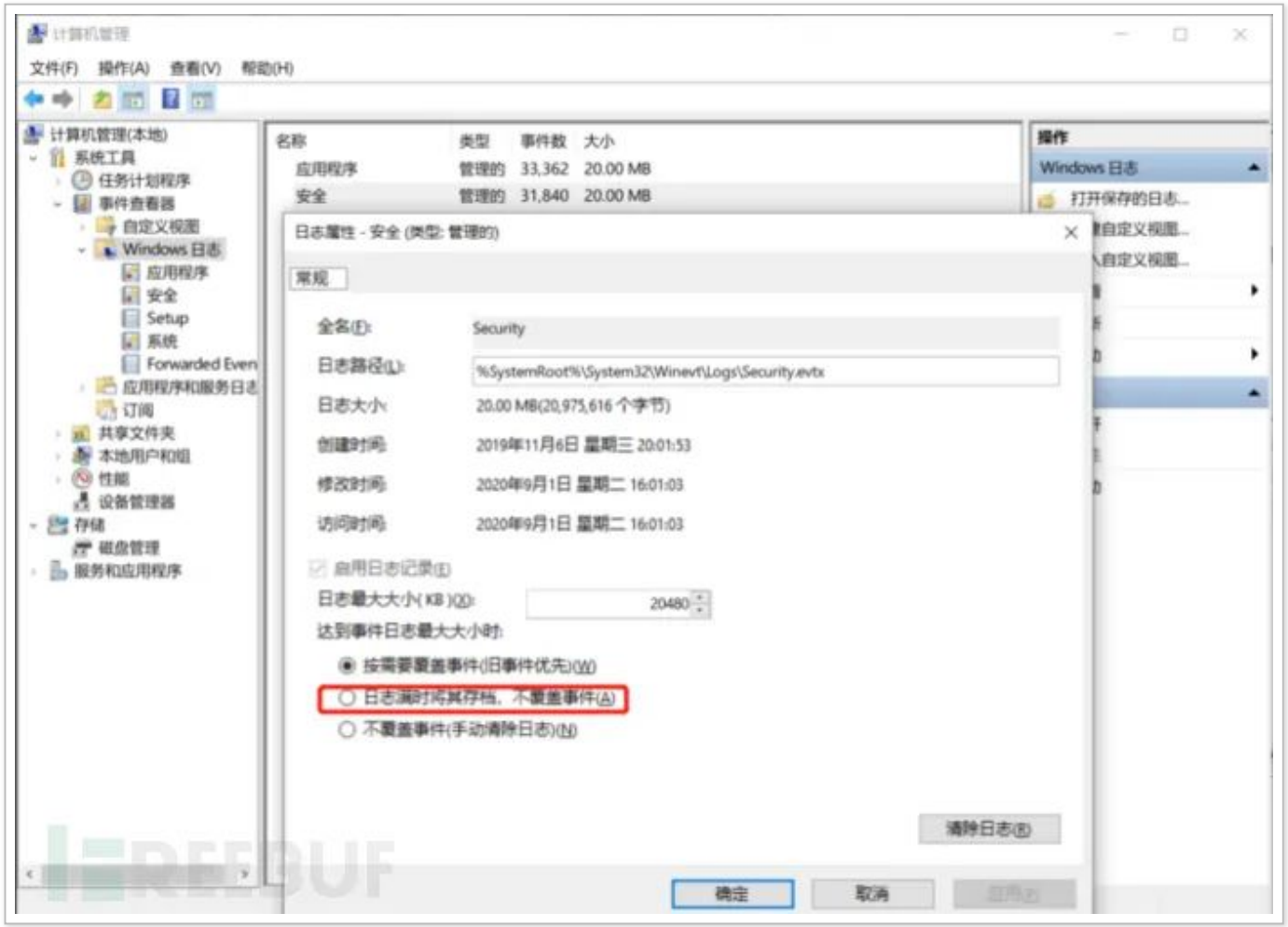
3.3 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等

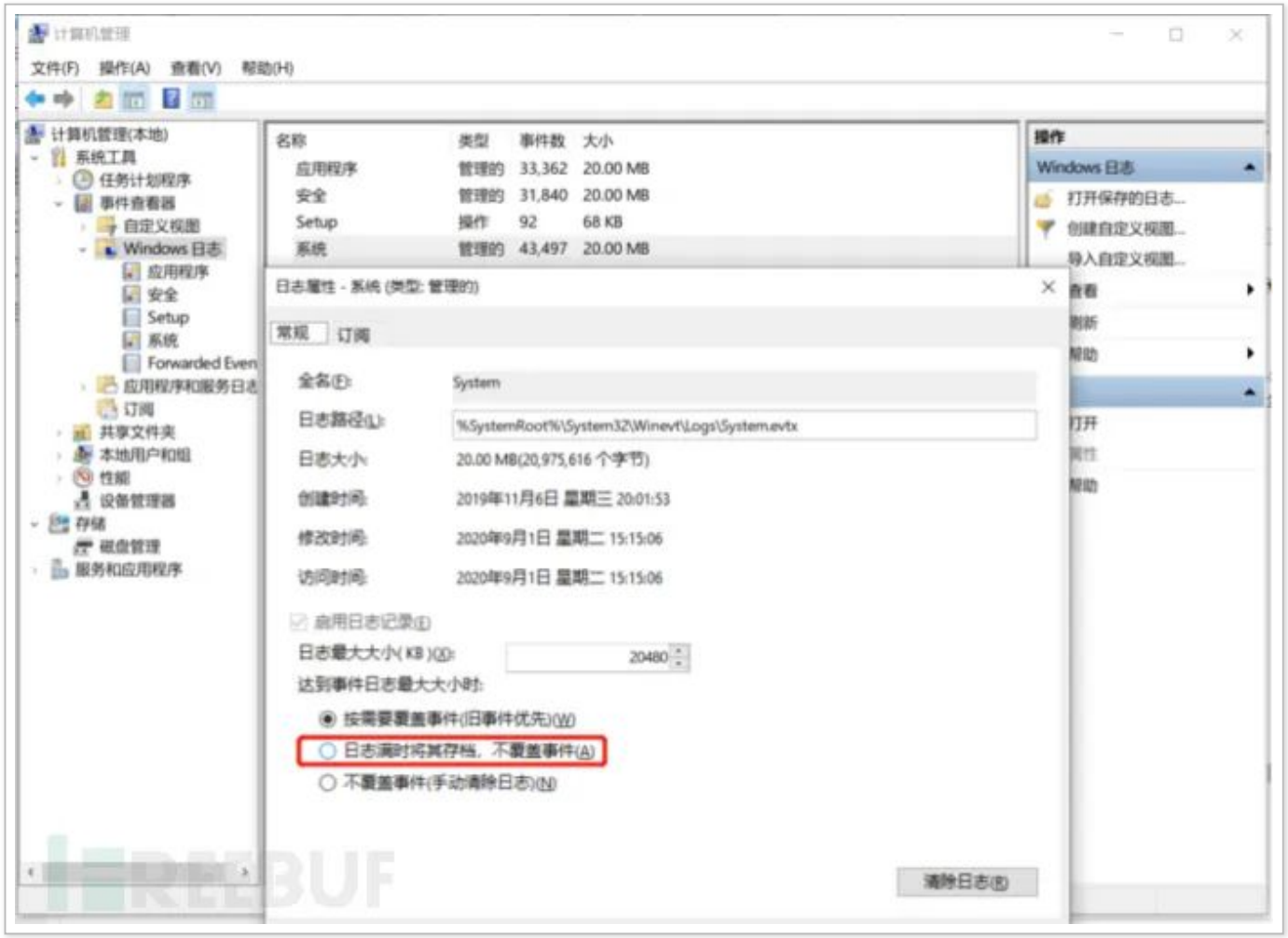
这里首先应该是查看审计记录文件的权限，是否会被未授权用户删除。

windows 中的日志一般我们比较关注应用程序日志、安全日志、系统日志（其中最重要的是安全日志），其存储文件分别是：

设置应用日志文件大小至少为 8192 KB，可根据磁盘空间配置日志文件大小，记录的日志越多越好。并设置当达到最大的日志尺寸时，按需要轮询记录日志：




计算机管理
文件(F) 操作(A) 查看(V) 帮助(H)
计算机管理(本地)
系统工具
任务计划程序
事件查看器
自定义视图
Windows 日志
应用程序
安全
Setup
系统
Forwarded Even
应用程序和服务日志
订阅
共享文件夹
本地用户和组
性能
设备管理器
存储
磁盘管理
服务和应用程序
名称 类型 事件数 大小
应用程序 管理的 33,362 20.00 MB
安全 管理的 31,840 20.00 MB
操作
Windows 日志
打开保存的日志...
日志属性 - 安全 (类型: 管理的)
常规
全名(F): Security
日志路径(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx
日志大小: 20.00 MB(20,975,616 个字节)
创建时间: 2019年11月6日 星期三 20:01:53
修改时间: 2020年9月1日 星期二 16:01:03
访问时间: 2020年9月1日 星期二 16:01:03
启用日志记录(E)
日志最大大小(KB)(X): 20480
达到事件日志最大大小时:
按需要覆盖事件(旧事件优先)(W)
日志满时将其存档，不覆盖事件(A)
不覆盖事件(手动清除日志)(N)
清除日志(R)
确定
取消



以上日志内容需要进行定期备份，审计记录保留至少 6 个月以上。

入侵防范

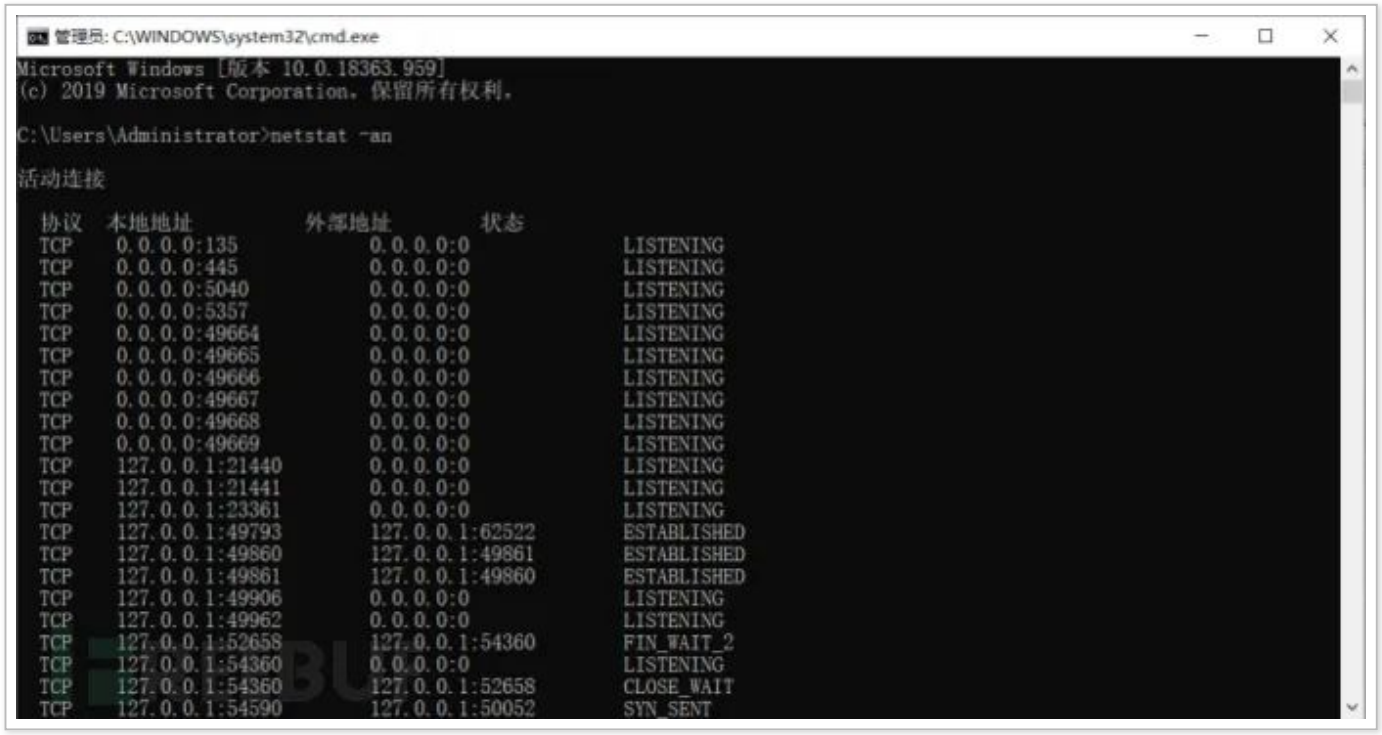
四、补丁修复

4.1 应遵循最小安装的原则，仅安装需要的组件和应用程序

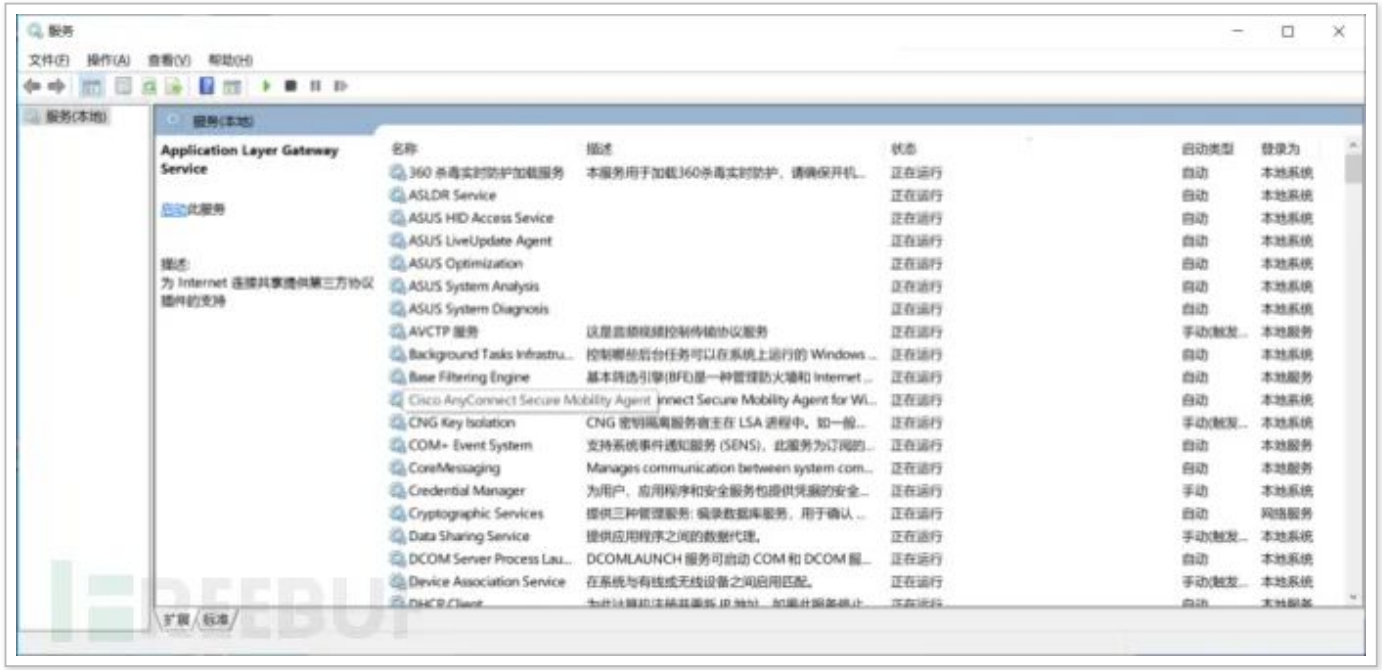
遵循最小安装原则，禁止 “夹带” 现象，只安装需要的组件和应用程序；

4.2 应关闭不需要的系统服务、默认共享和高危端口

使用 netstat -an 命令，查看开启了哪些端口：



查看所有的正在运行的服务



禁用 TCP/IP 上的 NetBIOS 协议，可以关闭监听的 UDP 137（netbios-ns）、UDP 138（netbios-dgm）以及 TCP 139（netbios-ssn）端口

停用不使用的服务

服务名称	建议
DHCP Client	如果不使用动态IP地址，就禁用该服务
Background Intelligent Transfer Service	如果不启用自动更新，就禁用该服务
Computer Browser	禁用
Diagnostic Policy Service	手动
IP Helper	禁用。该服务用于转换IPv6 to IPv4
Print Spooler	如果不需要打印，就禁用该服务
Remote Registry	禁用。Remote Registry主要用于远程管理注册表
Server	如果不使用文件共享，就禁用该服务。禁用本服务将关闭默认共享，如ipc$、admin$和c$等
TCP/IP NetBIOS Helper	禁用
Windows Remote Management (WS-Management)	禁用
Windows Font Cache Service	禁用
WinHTTP Web Proxy Auto-Discovery Service	禁用
Windows Error Reporting Service	禁用

4.3 启用 SYN 攻击保护

指定触发 SYN 洪水攻击保护所必须超过的 TCP 连接请求数阈值为 5。

指定处于 SYN_RCVD 状态的 TCP 连接数的阈值为 500。

指定处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值为 400。

操作步骤

打开 注册表编辑器，根据推荐值修改注册表键值。

Windows Server 2012

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect
推荐值：2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen
推荐值：500

Windows Server 2008

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SynAttackProtect
推荐值：2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxPortsExhausted
推荐值：5

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpen
推荐值：500

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpenRetried

推荐值：400

五、恶意代码防范

5.1 应安装防恶意代码软件或加固具有相应功能的软件，并定期进行升级和更新防恶意代码库

查看有无杀毒软件，是否升级为最新版本

六、数据备份恢复

6.1 应提供重要数据的本地数据备份与恢复功能

查看是否有备份文件，以及了解备份机制和恢复机制

若无，需要建立备份文件，进行每日增量、每周全量的备份策略。

6.2 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地

将备份文件存放异地且确保其有效性，避免出现单点故障后不具备恢复的风险。

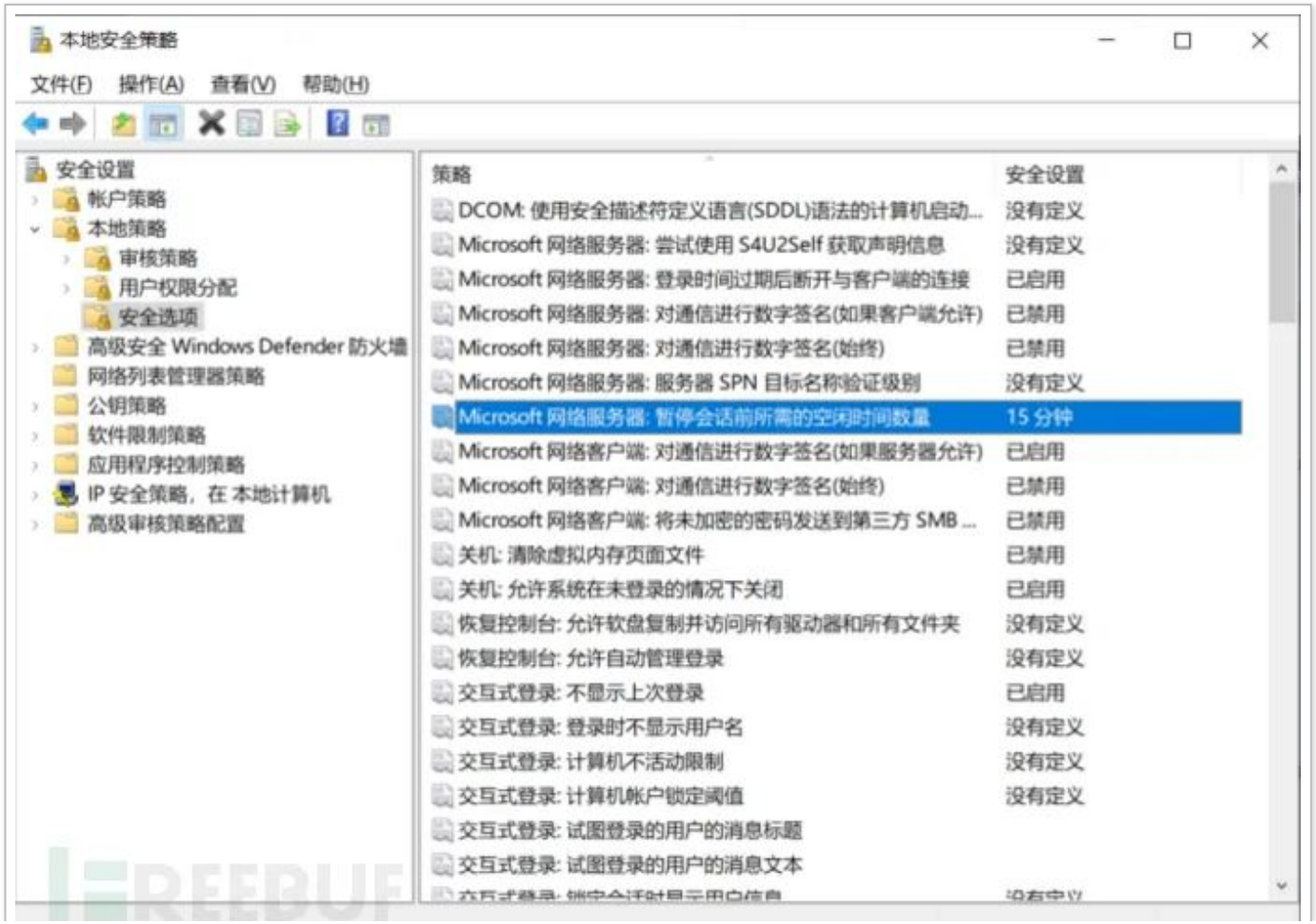
七、资源控制

7.1 应确保系统磁盘根分区已使用空间维持在 80% 以下

如果磁盘动态分区空间不足，建议管理员扩充磁盘容量

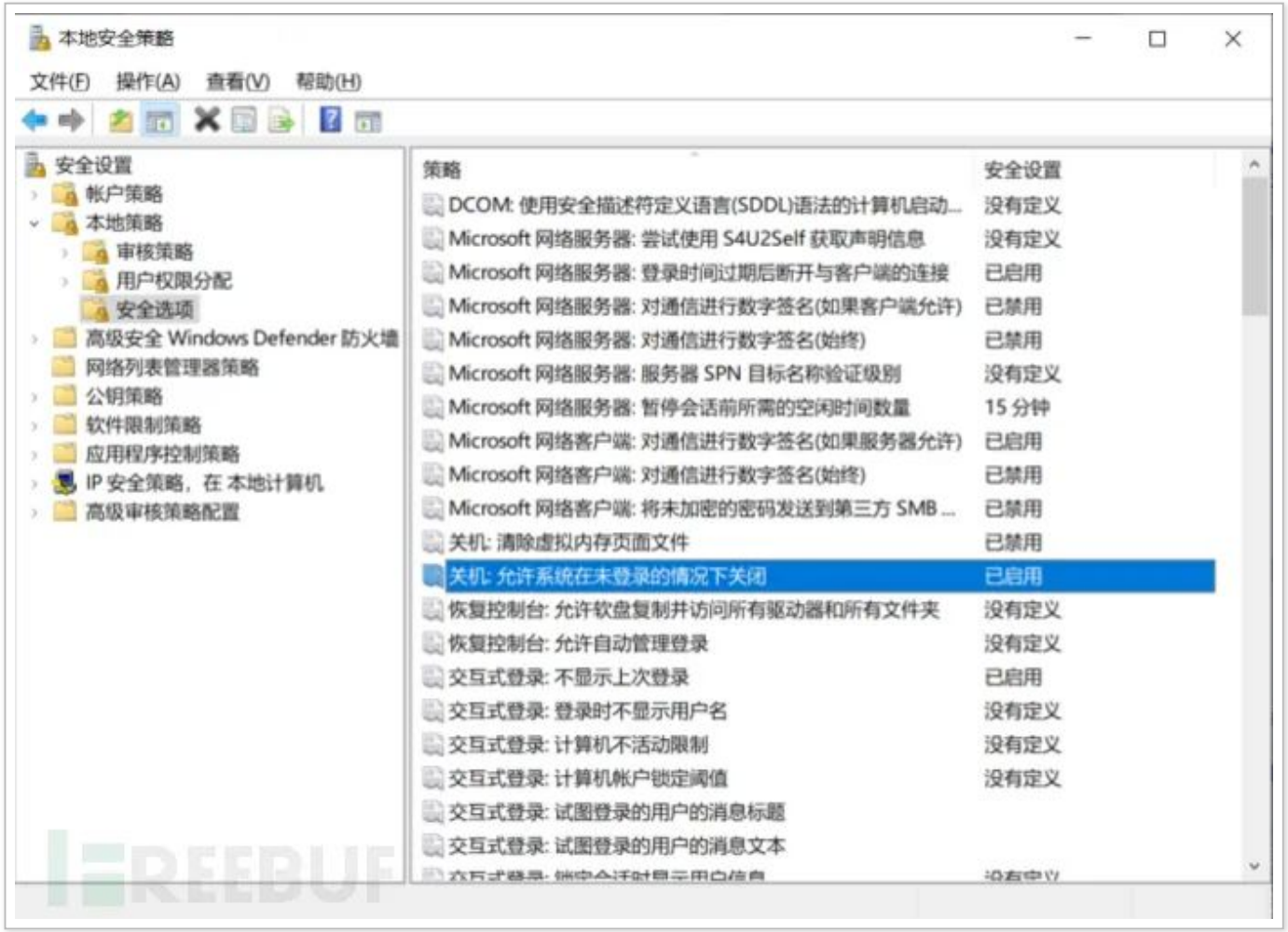
7.2 限制远程登录空闲断开时间

控制面板——管理工具——本地安全策略——安全选项：设置 15 分钟



7.3 禁用未登陆前关机

控制面板——管理工具——本地安全策略——安全选项：将已启用改为禁用



/